

Domande e risposte

Prendiamo con molta serietà l'impegno di difendere le informazioni che i clienti ci affidano e la loro privacy e per questo abbiamo implementato misure di sicurezza molto avanzate nelle nostre reti digitali.

Come molte altre agenzie governative e di altra natura, siamo però costantemente nel mirino di hacker che cercano di intromettersi nei nostri sistemi computerizzati per rubare informazioni sensibili. Purtroppo siamo stati recentemente vittime di un attacco del genere, un'intromissione nei nostri server.

Cosa è successo?

I nostri computer sono stati infettati da un virus (W32.QAKBOT) che si è propagato ai terminali del personale del Department of Unemployment Assistance (DUA), del Department of Career Services (DCS) e di alcuni One-Stop Career Center, a partire dal 19 aprile 2011 fino al 13 maggio 2011. Abbiamo preso provvedimenti immediati e, con l'aiuto della Symantec che ci fornisce i sistemi antivirus, abbiamo eliminato il virus dai nostri server e computer.

A quali dati potrebbero aver avuto accesso?

Con quel tipo di virus è possibile che siano stati asportati dati confidenziali degli utenti o del personale. Tali dati potrebbero comprendere nomi, numeri di previdenza sociale, indirizzi e-mail, indirizzi residenziali o di lavoro. Pensiamo che soltanto gli utenti che abbiano presentato una richiesta di sussidio nuova o richiesto l'assistenza del personale per la propria richiesta di sussidio o il personale che ha registrato richieste su carta nel suddetto periodo possano essere stati soggetti al furto di dati. Se ha consultato i Suoi dati online tramite DUA QUEST, WebCert o JobQuest e nessuno dei nostri operatori è stato coinvolto nell'operazione, i suoi dati sono rimasti al sicuro. Il virus è rimasto isolato nei nostri computer e non si è trasmesso a computer esterni che si siano collegati tramite le nostre applicazioni online.

Quali provvedimenti sono stati presi contro questa violazione?

Stiamo conducendo un'indagine interna per scoprire come questo incidente sia potuto avvenire e abbiamo incaricato alcuni esperti di applicare ulteriori misure di sicurezza per evitare che tutto ciò si ripeta. Stiamo anche lavorando con funzionari statali e federali per prevenire

future intromissioni e prenderemo ogni altro provvedimento per risolvere questo problema.

Ciò significa che sono stato vittima di un furto di identità?

No. Il fatto che qualcuno abbia avuto accesso alle Sue informazioni non significa necessariamente che ci sia stato un furto della Sua identità o che s'intenda usare i Suoi dati a scopo fraudolento. Volevamo solo informarla di quanto è accaduto e dei provvedimenti che abbiamo preso.

Cosa posso fare per proteggere i miei dati?

Avvertiamo tutti gli utenti online, quelli dei career center e gli imprenditori che presentano manualmente i loro rapporti di prestare molta attenzione alle loro informazioni personali e finanziarie. Chi ha richiesto l'aiuto di un nostro operatore, dal 19 aprile al 13 maggio, per accedere online al proprio file tramite DCS, DUA o un One-Stop Career Center è invitato ad applicare un avvertimento antifrode sui propri rapporti di credito.

Può richiedere un rapporto di credito gratuito o chiedere un avvertimento antifrode o il blocco del credito sul Suo file creditizio al consumo contattando uno degli uffici nazionali di informazioni creditizie. Una volta che l'ufficio di informazioni creditizie abbia posto l'avvertimento antifrode sul suo file creditizio, contatterà automaticamente anche gli altri due uffici. L'avvertimento antifrode resta in vigore, di solito, per 90 giorni ma può essere rinnovato. L'avvertimento antifrode sul proprio rapporto di credito è gratuito, mentre le agenzie di informazioni creditizie potrebbero addebitarle \$5.00 ogni volta che applicano o rimuovono il blocco del credito. I rapporti di credito sono disponibili gratuitamente una volta ogni 12 mesi da ciascuna delle compagnie di rendicontazione del credito. Gli uffici di credito possono essere contattati come segue:

Equifax: (800) 525-6285 (<http://www.equifax.com>)

Experian: (888) 397-3742 (<http://www.experian.com>)

TransUnion: (800) 680-7289 (<http://www.tuc.com>)

Può anche ottenere ulteriori informazioni nel nostro sito <http://1.usa.gov/jcLaDY> sul furto di identità e su come proteggere i propri dati personali, chiamando il numero **1-877-232-6200** al EOLWD.

Sarò contattato da funzionari statali che mi chiederanno dati personali, in seguito a questo incidente?

Noi non contattiamo gli utenti per chiedere loro dati personali quali il numero di previdenza sociale, della carta di credito o del conto bancario. Se riceve telefonate o e-mail che le chiedono informazioni personali di questo tipo, le denunci subito al Distretto di Polizia più vicino o all'Ufficio del Procuratore Distrettuale o all'Ufficio del Procuratore Generale.

Cosa devo fare se ritengo di essere stato vittima di un furto di identità?

Se crede di essere stato vittima di un furto di identità dovrebbe denunciare il fatto alla più vicina stazione di Polizia. Se ritiene, inoltre, che i Suoi dati personali siano stati usati a scopo di assunzione, ne informi l'Internal Revenue Service (IRS) e la Social Security Administration (SSA).